

REMARKS

The Examiner has rejected Claims 1-2, 4-11, and 13-20 under 35 U.S.C. 103(a) as being unpatentable over Nachenberg (U.S. Patent No. 6,357,008) in view of Serbinis et al. (U.S. Patent No. 6,314,425). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to at least substantially include the subject matter of former dependent Claims 2 and 6 et al.

With respect to each of the independent claims, the Examiner has relied on the following excerpts from the Nachenberg reference to make a prior art showing of applicant's claimed "structured virus database storing one or more virus definition records" (see this or similar, but not necessarily identical language in each of the independent claims).

"Signature scanning antivirus programs work by scanning files for signatures of known viruses. A signature is a sequence of bytes that may be found in a virus program code, yet is unlikely to be found elsewhere. To "extract" a signature, an antivirus researcher must analyze the virus. Once this signature is determined, it is recorded in a database of virus signatures to be used by an antivirus program." (Col. 1, lines 27-33)

"...positive" rate if properly implemented. However, only viruses whose signatures have already been determined and stored in the signature database may be detected using signature scanning. Moreover, the signature database must be updated frequently to detect the latest viruses." (Col. 1, lines 42-45)

The Nachenberg reference teaches a database of virus signatures. Applicant, however, claims a "structured virus database storing one or more virus definition records" (emphasis added). These definition records claimed by applicant further comprise at least an identifier, virus name, and virus definition, and removal sentences, whereas the Nachenberg's virus signatures merely consist of "a sequence of bytes that may be found in a virus program code, yet is unlikely to be found elsewhere" (Col. 1, lines 28-30). As a result, applicant's claims are clearly distinct.

- 9 -

Additionally, with respect to each of the independent claims, the Examiner has relied on the following excerpt from the Nachenberg reference to make a prior art showing of applicant's claimed "at least one virus name associated with the computer virus" (see this or similar, but not necessarily identical language in each of the independent claims).

"...designed to be specific to a single virus. Instead, they are meant to be as general as possible in order to detect the operation of many different viruses." (Col. 2, lines 43-45)

The above reference teaches the searching of a target program for sequences of instructions not specific to a specific virus. This is completely unrelated to applicant's claimed "at least one virus name associated with the computer virus" (emphasis added). Additionally, it is stated in the Nachenberg reference that the sequences of instructions are "unlike [the] virus signatures" described earlier (Col.2, line 42). Thus, even if applicant's claimed virus name were to be equated to Nachenberg's sequences of instructions, it is impossible, in Nachenberg, for a database of virus signatures to contain the sequences of instructions, as they were contrasted in the reference. Since applicant's claimed virus name is not found in Nachenberg, and is also a component of applicant's claimed virus definition record, it is clearly distinct.

Furthermore, with respect to each of the independent claims, the Examiner has relied on the following excerpt from the Nachenberg reference to make a prior art showing of applicant's claimed "virus removal sentence comprising object code providing operations to clean the identified computer virus from the computer system" (see this or similar, but not necessarily identical language in each of the independent claims).

"A signature scanning antivirus program can identify particular virus strains for removal and may have a low "false-positive" rate if properly implemented. However, only..." (Col. 1, lines 39-41)

- 10 -

The above reference teaches the identification of virus strains for removal. Applicant's claim, however, requires the actual "object code providing operations to clean the identified computer virus from the computer system" (emphasis added). Since the reference only teaches the identification of viruses for removal and does not provide any operations for such cleaning, applicant's claim is clearly distinct.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to further distinguish applicant's claim language from the above reference, as follows:

"converting each virus definition set in the virus data file into a virus definition record"; and

"accessing the virus definition records in the structured virus database to perform at least one of adding, removing, and replacing a virus definition record" (see these or similar, but not necessarily identical language in each of the independent claims).

- 11 -

With respect to the subject matter of former Claim 2 (now at least substantially incorporated into each of the independent claims), the Examiner has relied on the following excerpts from the Nachenberg reference to make a prior art showing of applicant's claimed client anti-virus language decompiler for "converting each virus definition set in the virus data file into a virus definition record" (see this or similar, but not necessarily identical language in each of the independent claims).

"Non-integrity-based (also called "heuristic") unknown virus detection is used to detect new and unknown viruses without any integrity information. A heuristic antivirus program examines a target program (executable file, boot record, or possibly document file with a macro) and analyzes its program code to determine if the code appears virus-like. If the target program's code appears virus-like, then the possible infection is reported to the user." (Col. 2, lines 18-25)

"A signature scanning antivirus program can identify particular virus strains for removal and may have a low "false-positive" rate if properly implemented. However, only viruses whose signatures have already been determined and stored in the signature database may be detected using signature scanning. Moreover, the signature database must be updated frequently to detect the latest viruses." (Col. 1, lines 39-45)

The above excerpt from Nachenberg teaches the analysis of program code to determine if it appears virus-like, as well as signature scanning of a frequently updated signature database. On the other hand, applicant's claim requires the conversion of a virus definition set, comprising binary data coding instructions to detect and clean computer viruses, into a virus definition record, comprising an identifier, at least one virus name, and virus definition, and removal sentences, all of which are not mentioned in the prior art, when taken in combination as claimed. The analysis of code and the scanning of a signature database of Nachenberg simply does not meet applicant's claimed conversion of binary data coding instructions into an identifier, at least one virus name, and virus definition and removal sentences. As a result, applicant's claim is clearly distinct.

Additionally, with respect to the subject matter of former Claim 6 (now at least substantially incorporated into each of the independent claims), the Examiner has relied

- 12 -

on the following excerpts from the Nachenberg reference to make a prior art showing of applicant's claimed database engine for "accessing the virus definition records in the structured virus database to perform at least one of adding, removing, and replacing a virus definition record." (see this or similar, but not necessarily identical language in each of the independent claims).

"signature scanning. Moreover, the signature database must be updated frequently to detect the latest viruses." (Col. 1, lines 44-45)

The above reference teaches the updating of a signature database. In contrast, applicant's claim requires accessing the virus definition records in the structured virus database in order to perform at least one of adding, removing, and replacing a virus definition record. Also, as mentioned above, a virus definition record differs greatly from the above reference's virus signature. As a result, applicant's claims are clearly distinct.

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

- 13 -

Commissioner is authorized to charge any additional fees or credit any overpayment to
Deposit Account No. 50-1351 (Order No. NAI1P376/00.140.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100